



BROADWATER
CHURCH OF ENGLAND
PRIMARY SCHOOL

Rectory Gardens
Worthing
West Sussex
BN14 7TQ

TEL 01903 235389
EMAIL office@broadwaterce.org

www.broadwater.w-sussex.sch.uk

Online Safety Policy (2023-2024)

This policy is derived from the SWGfl 2022 (South West Grid for Learning)
Model School Online Safety Policy

Turn your ear to wisdom and apply your heart to understanding (Proverbs 2:2)

Broadwater is a Christian School. We will enable children to become wise, confident, successful learners with the motivation, skills and responsibility to make a positive difference in God's world. Our vision is underpinned by the values we live by.

The Holy Spirit produces this kind of fruit in our lives: love, joy, peace, patience, kindness, goodness, faithfulness, gentleness, and self-control. There is no law against these things! Galatians 5:22

It is this fruit that, in partnership with parents, we will instil in the children of our school.

Contents

Development/Monitoring/Review of this Policy 3

Roles and Responsibilities..... 3

Policy Statements including Mobile Technology 6

Communications 11

Dealing with unsuitable/inappropriate activities 13

Responding to incidents of misuse 15

Illegal Incidents 16

Other Incidents..... 17

School actions and sanctions..... 17

Appendix..... 20

Development/Monitoring/Review of this Policy

This Online Safety Policy has been developed by a working group made up of: Teachers and Governors.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body (safeguarding governor) has taken on the role of Online Safety and has regular meetings with the Headteacher (once a term).

- reporting to relevant Governor committees.
- Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see appendix for flow chart on dealing with online safety incidents and “Responding to incidents of misuse” and relevant Local Authority disciplinary procedures). *Online Safety BOOST (see West Sussex Services for schools) includes an ‘Incident Response Tool’ (and forms to complete) that outlines the steps any staff facing an issue, disclosure or report, need to follow.*
- Headteacher/Senior Leadership Team will monitor if any reports on Online Safety are generated.

Online Safety Lead (Headteacher)

- leads the Online Safety training (with support from colleagues)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs

Incidents will be dealt with by the Headteacher

Network Manager/Technical staff

Those with technical responsibilities monitored by Headteacher are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement on recruitment/update of policy (Acceptable Users Policies AUP / Acceptable Use Agreement AUA)
- they report any suspected misuse or problem to the Headteacher for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead/Designated Person/Officer

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

(N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. At Broadwater all staff have a safeguarding responsibility which includes online safety.

DSL and Staff

The Headteacher (DSL) will also be responsible for regular reporting to the Governing Body.

Those responsible for online safety are: DSLs, Headteacher, School Bursar, teaching staff, IT technicians and support staff.

- The production/review/monitoring of the school online safety policy/documents- teaching staff
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression- teachers/subject leader
- monitoring network/internet/filtering/incident logs- technicians
- consulting stakeholders – including parents/carers and the pupils about the online safety provision- Senior leadership and teachers.

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations-KS2
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so – all pupils
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school if related to their membership of the school

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through parents' meetings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education –Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum should be provided as part of Computing/PHSE (RHE/RSE) other lessons and should be regularly revisited:

- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Headteacher/Subject lead will review guidance documents released by relevant organisations.
- This Online Safety Policy, and its updates, will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Headteacher/ Subject lead will provide advice/guidance/training to individuals as required.

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Participation in school Safeguarding training/information sessions for Governors
- Prevent training
- Technical – infrastructure/equipment, filtering and monitoring - IT technicians
- It is the school's responsibility to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below (see technical support policies). It is also important that the managed service provider is fully aware of the school online safety policy/acceptable use agreements. The school should also check their Local Authority policies on these technical issues (model policies used).

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users have a shared log in user name and password for their year group. For online learning platforms they have their own username and password. Users are responsible for the security of their username and password.
- The “administrator” passwords for the school systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe)

- Technical support is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. – IT technicians.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”).
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users – staff/pupils).
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- Users to report any actual/potential technical incident/security breach to the Headteacher, as agreed.
- Appropriate security measures are in place (IT technicians) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place (Staff and Volunteers Acceptable Use of the Internet policy) for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (Staff and Volunteers Acceptable Use of the Internet policy) regarding the extent of personal use that users (staff/pupils) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (Staff and Volunteers Acceptable Use of the Internet policy) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (Staff and Volunteers Acceptable Use of the Internet policy)) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technology

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud- based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy,

behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

- The school acceptable use agreements for staff, pupils and parents/carers will consider the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned (including student teachers)	Visitor owned
Allowed in school	No	Yes	No	N/A	Yes, not to be used in class time-see handbook.	Yes Switched off
Full network access	No	Yes	No		No	No
Internet	Yes	Yes	Yes		Yes	No
Network access	Partial drive access	Partial drive access	Partial drive access		No	No
Remote access for teachers	Yes	Yes	Yes		Yes	No

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press (Acceptable Use Agreement signed by parents or carers at the start of the year - see parents/carers acceptable use agreement in the appendix and Enrolment Booklet).
- In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any

activities involving other pupils in the digital/video images. (Referenced on page 3 of the parent/carer used agreement.)

- Within school, Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes (selected staff permitted).
- If we receive a request to use your child's image (photograph) from an external body we would seek permission for this.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images and the parent/carers consent form will be checked.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers (see appendix for parent consent form).

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the appendices to this document. Schools should ensure that they take account of policies and guidance provided by local authorities.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for.

Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear School Privacy Notice.
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see/to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter (yearly). Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects (pupils) understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Staff & other adults	Students/Pupils
----------------------	-----------------

	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to the school		/						
Use of mobile phones in lessons				/				
Use of mobile phones in social time	/							
Taking photos on mobile phones/cameras			/		/ cameras			
Use of other mobile devices e.g. tablets	/				/			
Use of personal email addresses in school, or on school network				/				
Use of school email for personal emails	/							
Use of messaging apps		/						
Use of social media		/						
Use of blogs						/		

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the nominated person– in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, website, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

(See Social Media Policy 2022- 2023)

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X

material, remarks, proposals or comments that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						
<ul style="list-style-type: none"> • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) 						X
N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	

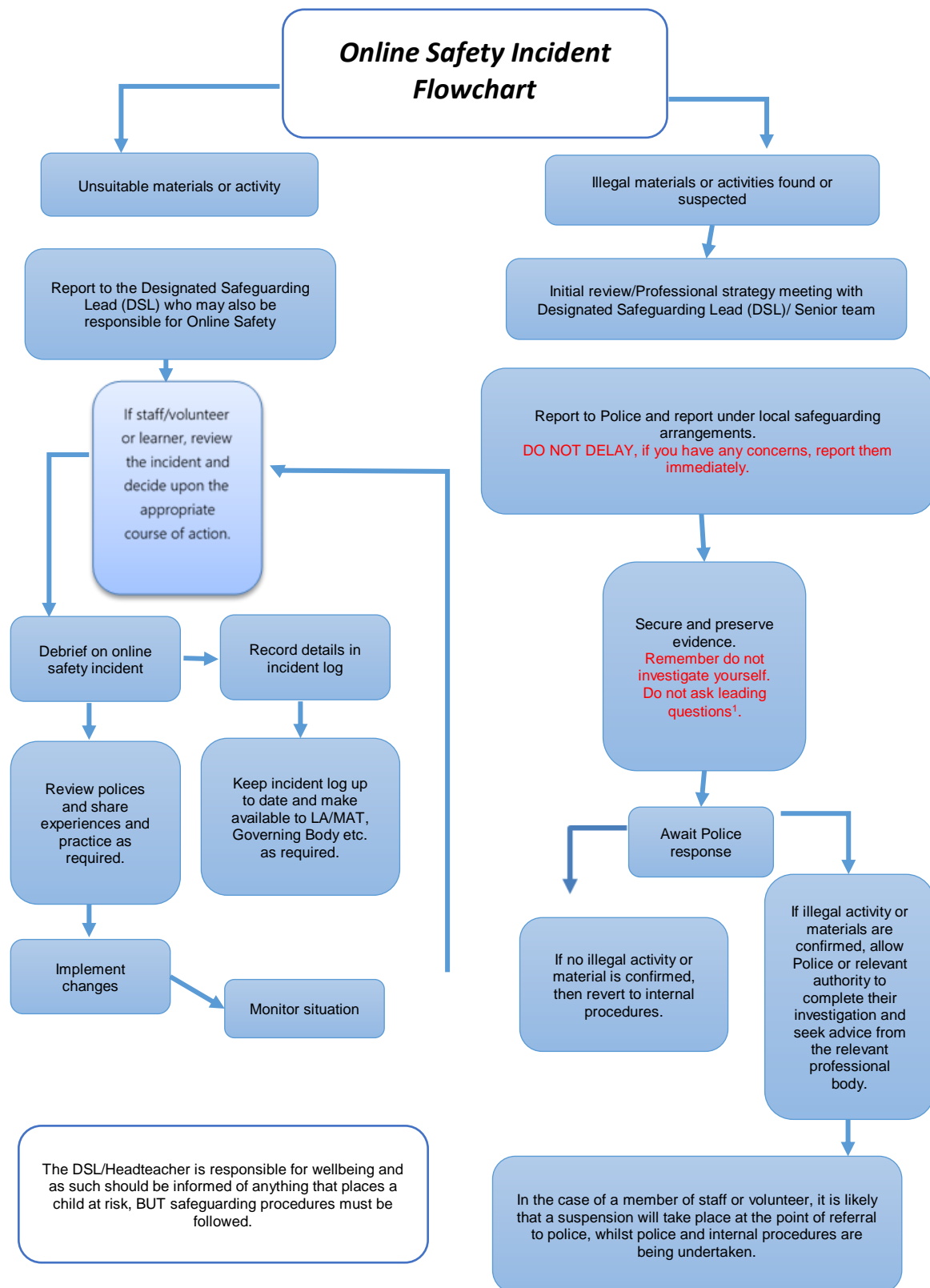
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		x			
On-line gaming (non-educational)			x		
On-line gambling				x	
On-line shopping/commerce (non-educational)				x	
File sharing			x		
Use of social media			x		
Use of messaging apps			x		
Viewing of video broadcasting e.g. Youtube (teacher access only) Material not to be shared on Youtube		x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and, if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority Group or national/local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - offences under the Computer Misuse Act (see User Actions chart above)
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the LA for evidence and reference purposes.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Actions/Sanctions

Pupils Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X		x			
Unauthorised use of non-educational sites during lessons	x							
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	x	x			x			
Unauthorised/inappropriate use of social media/messaging apps/personal email	x	x			x			
Unauthorised downloading or uploading of files	x	x		x				
Allowing others to access school network by sharing username and passwords		x		x				
Attempting to access or accessing the school network, using another pupil's account	x			x				
Attempting to access or accessing the school network, using the account of a member of staff		x			x			
Corrupting or destroying the data of other users		x			x			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x			x			
Continued infringements of the above, following previous warnings or sanctions		x			x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x			x	x	x	x
Using proxy sites or other means to subvert the school's filtering system		x			x	x	x	x

Accidentally accessing offensive or pornographic material and failing to report the incident		x				x	x	x	
Deliberately accessing or trying to access offensive or pornographic material		x				x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		x				x	x	x	x

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email		x				x		
Unauthorised downloading or uploading of files		x						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		x					x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner		x						
Deliberate actions to breach data protection or network security rules		x			x		x	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x			x		x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x					x	x

Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils	x	x						x
Actions which could compromise the staff member's professional standing	x	x						x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x					x	
Using proxy sites or other means to subvert the school's filtering system		x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	x			
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x			x	x		
Continued infringements of the above, following previous warnings or sanctions	x	x						x

If these incidents involved SLT then the concern must be taken to the Chair of Governors.

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe online safety self-review tool: Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use. Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from: SWGfL Online Safety Policy Templates West Sussex Services for Schools 2020

Appendices

- Safe Use of Children’s Photographs and Video Information..... 22
- Consent Form for Photographs and Videos (use of images and videos) 23
- Responding to incidents of misuse – flow chart..... 24
- Record of reviewing devices/internet sites (responding to incidents of misuse)..... 25
- Reporting Log..... 26
- School Personal Data Advice and Guidance..... 28
- Legislation..... 42
- Glossary of Terms..... 49

Safe Use of Children's Photographs and Video

Taking, keeping and publishing photographs and video footage involves processing personal data. The School's Privacy Notice will cover the majority of processing where it is limited to official use, monitoring and for educational purposes. However, to comply with the Data Protection Act and the General Data Protection Regulations, consent **will** be required where there is additional processing of personal data which is not within the reasonable expectation of those involved, such as taking photographs for certain media use.

The use of photography and video within the school is an essential part of the regular curriculum work of the school. This includes, for example, the use of these media for assessment purposes, recording of work in topic books and for internal celebration of work on displays. We may occasionally use video containing your child to share good educational practice with teachers. In these instances, we will adhere strictly to the rules on using photographs outlined in our policy.

Broadwater Church of England Primary School would like to take photographs and or video recordings of pupils whilst they attend the school to celebrate their achievements and successes. Still or moving images may be published in our printed publications (e.g. School brochure, newsletters) and/or on our school external website. They may also be used to promote the good educational practice of the school to other teachers, e.g. at training events organised by the school, Local Authority or national education/government institutions. Children's full names will never be published alongside their photograph external to the school. Names may be used internally, for example – on a display. Photographs/videos may also be published for *internal use only*, as part of children's regular classroom work e.g. on classroom displays, within multimedia projects (e.g. PowerPoint), on the school's internal network and to share educational achievements with parents, e.g. video presentation of a school trip. Electronic images, whether photographs or videos, will be stored securely on the school's network which is accessible only by authorised users. Promotional materials including photographs may continue to be used once a child has left the school until such time that these materials are updated e.g. website photographs and brochure photographs.

Before using any photographs/videos of children parental permission is sought. This is by means of the School Enrolment Booklet new parents complete prior to their child's entry to the school. This consent is valid from the date of signing until your child leaves the school.

Photographs and videos may be securely archived after your child has left the school. Archiving provides a valuable record of the school's history for future generations. On an occasional basis, such as a published historical record of the school or new publicity material where a specific photograph illustrates clearly an aspect of school, a photograph may be re-used or re-published. If we receive a request to use your child's image (photograph) from an external body we would seek permission for this.

We recognise that parents, carers and family members will wish to record events such as school plays, sports days etc. to celebrate their child's achievements. Broadwater is happy to allow this on the understanding that such images/recordings are used purely for personal family use and not posted to any public social media.

Please note that photographs may be taken at public events/performances by third parties beyond our control.

Consent Form for Photographs and Video

Child's Name:	Date of Birth:
---------------	----------------

By signing this form, you consent to the use of photographs/video/work of your child for the following purposes:

**Please circle clearly
your answer**

1	I give permission for my child's photograph to be used in printed publications (e.g. school handbook) produced by Broadwater Church of England Primary School.	YES	NO
2	I give permission for my child's photograph to be used on the school website or other school-hosted media site as part of a large group or whole school activity (e.g. productions and sport's events).	YES	NO
3	I give permission for my child's photograph to be used on the school website or other school-hosted media site showing an individual activity? (e.g. holding a winner's trophy).	YES	NO
<i>(Please note that the above is a very important way of promoting the activities of the school and celebrating the many wonderful achievements of our children. The school would greatly appreciate your full support for this.)</i>			
4	I give permission for my child's photograph to be used by external media (e.g. newspaper other organisation's websites). This might be as part of a school team/class or record of a school event.	YES	NO
5	I give permission for my child to have their school photograph taken, individually and in classes for purchase by parents/carers either digitally or printed and for recordings to be taken (e.g. a school play) which will be available for purchase by parents/carers.	YES	NO

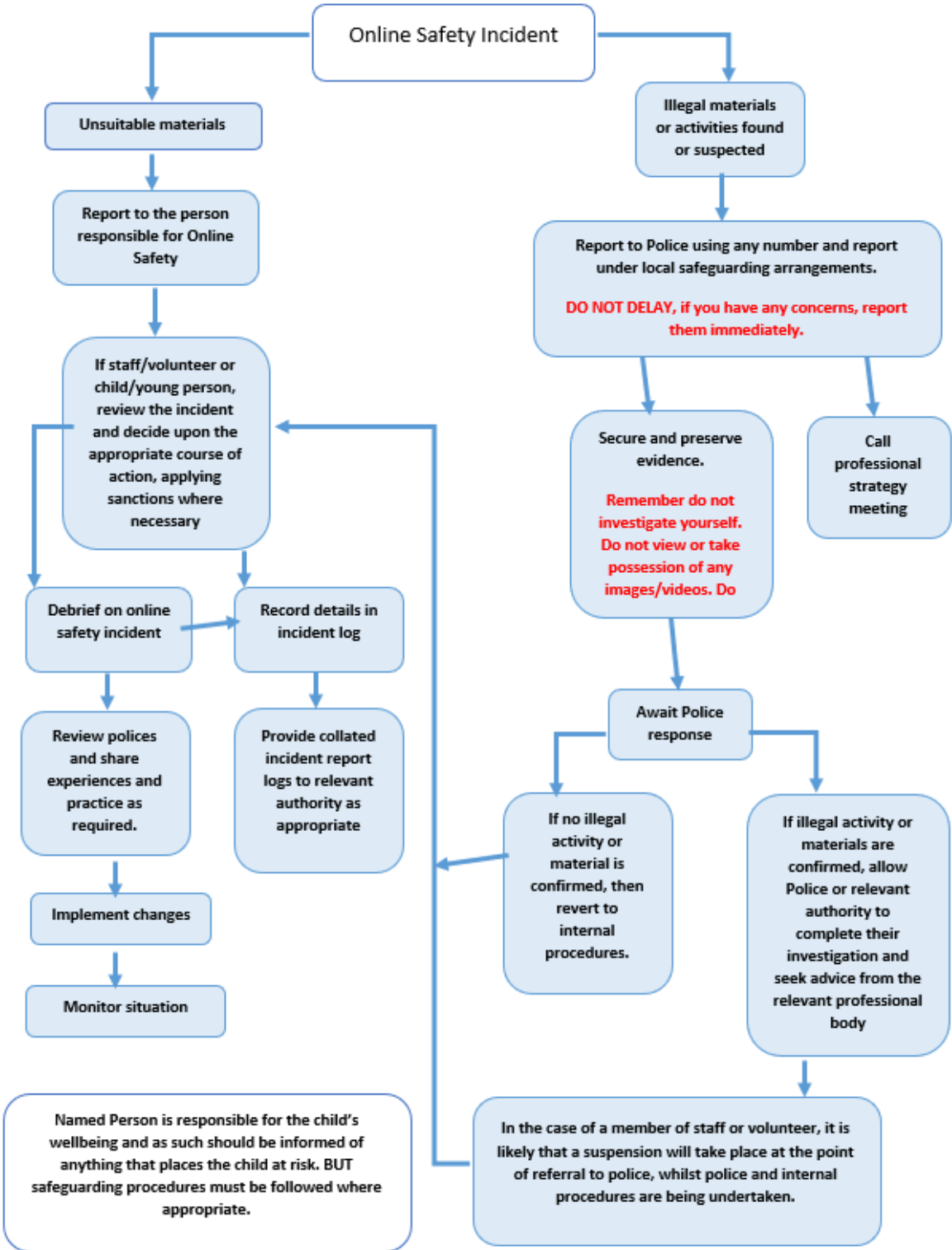
We regard the use of photography and video within the school as an essential part of the regular curriculum work of the school. This includes, for example, the use of these media for assessment purposes, recording of work in topic books and for internal celebration of work on displays. We may occasionally use video containing your child to share good educational practice with teachers. In these instances, we will adhere strictly to the rules on using photographs outlined in our policy.

The school owns the copyright of this photograph/video. It will be used solely for the purpose/s mentioned above.

You have the right to opt out or withdraw consent in respect of one or all of these options at any time. Should you wish to withdraw your consent you will need to notify the Data Protection officer (DPO) in writing using the school address or email DPO@broadwaterce.org. Alternatively, please complete a new form and we will update our records accordingly. Opting out will be effective from that date only and will not be retrospective.

Signed: Parent/Guardian	Date:
Please confirm you have parent/legal responsibility YES / NO	
Print Name:	

Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

School:
Date:
Reason for investigation:
.....
.....

Details of first reviewing person

Name:
Position:
Signature:

Details of second reviewing person

Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

School:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

School:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Further Guidance

Schools may wish to seek further guidance. The following is recommended:

Schools in England (and Wales) are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering” (Revised Prevent Duty Guidance: for England and Wales, 2015).

The Department for Education ‘Keeping Children Safe in Education’ requires schools to: “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system” however, schools will need to “be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

In response UKSIC produced guidance on – information on “Appropriate Filtering”

West Sussex Guidance for schools – questions for technical support – this checklist is particularly useful where a school uses external providers for its technical support/security.

School Personal Data Advice and Guidance

Data Protection Law – A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 – this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as; how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc. In this document the term “Data Protection Law” refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a ‘data controller’.

A school/academy is, for the purposes of the Data Protection Law, a “public body” and further processes the personal data of numerous data subjects on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools/academies is available on the Information Commissioner’s Office (ICO) website including information about the Data Protection Law.

The ICO’s powers are wide ranging in the event of non-compliance and schools/academies must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to data subjects;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the school/academy to put in place appropriate privacy notices (to give a data subject information about the personal data processing activities, legal basis of processing and data subject rights) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

Data Mapping to identify personal data, data subjects and processing activities

The school and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school has a data map of these activities; it can then make sure that the correct privacy notices are provided, put in place security measures to keep the personal data secure and other steps to avoid breach and also put in place data processing agreements with the third parties.

The data map should identify what personal data is held in digital format or on paper records in a school, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors – and personal data of names, addresses, contact details
- Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEND reports
- Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as ‘special category’ being personal data; “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”

This should be identified separately and to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

The school will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

- (a) Consent: the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)
- (b) Contract: the processing is necessary for a contract you have with the data subject
- (c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) Vital interests: the processing is necessary to protect someone’s life.
- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities' use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.

Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a school is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.

- if your school or academy requires learner details to be stored in a Management Information System (MIS), it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is
- What personal data is being processed and the lawful purpose of this processing
- where and how the personal data was sourced
- to whom the personal data may be disclosed
- how long the personal data may be retained
- data subject's rights and how to exercise them or make a complaint

In order to comply with the fair processing requirements in data protection law, the school will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – unlikely to be used in a school/academy context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and academies, such as the right of access. You need to put procedures in place to deal with Subject Access Requests. These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

A school must not disclose personal data even if requested in a Subject Access Request; if doing so would cause serious harm to the individual

- child abuse data
- adoption records
- statements of special educational needs

Your school must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high-profile issue for schools, academies and other organisations. It is important that the school/academy has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school will want to avoid the criticism and negative publicity that could be generated by any personal data breach

Schools have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

Schools will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

All significant data protection incidents must be reported through the DPO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you must notify the ICO; if it’s unlikely then you don’t have to report it. You do not need to report every breach to the ICO.

The school/academy should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- “responsible person” for each incident
- communications plan, including escalation procedure

- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

Secure storage of and access to data

The school should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school/academy equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school/academy personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school/academy policy once it has been transferred or its use is complete.

The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school systems, including off-site backups.

The school should have clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act.

The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their

home), they should preferably have secure remote access to the management information system or learning platform

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of personal data

The school should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society Toolkit for schools provides support for this process. The school must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school to target training at the most at-risk data
- record any breaches that impact on the personal data

Fee

The school should pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the school to a penalty in addition to other fines possible under the Data Protection Law.

Responsibilities

Every maintained school is required to appoint a Data Protection Officer as a core function of 'the business' – School Business Manager

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with Data Protection Law

The school may also wish to appoint a Data Manager. Schools are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- oversee the System Controllers

The school may also wish to appoint a System Controller (School Business Manager) for the various types of data being held (e.g. learner information / staff information / assessment data etc.). System Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school or elsewhere if on school business).

Training & awareness

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controller

Freedom of Information Act

All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school/academy to consider whether the requested information should be released into the public domain. FOI links to Data Protection Law whenever a request includes personal data. Good advice would encourage the school/academy to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/academy's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- ensure that a well-managed records management and information system exists in order to comply with requests
- ensure a record of refusals and reasons for refusals is kept, allowing the school/academy to review its access policy on an annual basis

Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a model publication scheme which they should complete. The school's publication scheme should be reviewed annually.

The ICO produce guidance on the model publication scheme for schools. This is designed to support schools complete the Guide to Information for Schools.

Parental permission for use of cloud hosted services

Schools that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Policy Statements

Pupils, up to year 4, are not allowed to bring mobile phones or other personal electronic devices into school they are not allowed to use them on school property. Year 5 and 6 pupils may bring a mobile device to school but must turn it off on entry to school site.

If pupils breach these rules:

They will be given a warning on the first time. However, if they do this again then their phone will be confiscated and parents will have to come into the school to collect the device.

Authorised staff (Headteacher and Deputy Headteacher) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone/personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of pupils.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the pupil to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags. (Schools will need to take account of their normal policies regarding religious garments/headwear and may wish to refer to it in this policy)

A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data/files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart (West Sussex Services for Schools) Local authorities/local safeguarding partnerships may also have further guidance, specific to their area.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the

data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should know who to contact, within school, for further guidance before taking action and that the person or persons is or are named within this policy).

A record should be kept of the reasons for the deletion of data/files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices).

(See relevant section of the Behaviour Policy which may assist in covering the school against damage/loss claims.)

Audit/Monitoring/Reporting/Review

The responsible person (The Headteacher) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data/files. (See appendix for a template log sheet.)

These records will be reviewed by the Headteacher and the safeguarding governor, termly. This policy will be reviewed by the Headteacher and governors annually and in response to changes in guidance and evidence gained from the records.

The school is required to publish its Behaviour Policy to parents annually (including on its website). (DfE guidance can be found at: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>.)

Mobile Technologies Policy (Inc. BYOD/BYOT: bring your own devices/technology)

Mobile technology devices may be school owned/provided by or a privately-owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the pupils, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned or personally owned. The mobile technologies policy should sit alongside a range of policies including but not limited to the safeguarding policy, anti-bullying policy, acceptable use agreements, policies around theft or malicious damage and the behaviour policy.

Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in pupils that will prepare them for the high tech world in which they will live, learn and work.

Considerations (Not all applicable to Broadwater currently)

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

A range of mobile technology implementations is possible. The school should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies
- The school allows: (see table on page 12)

When personal devices are permitted (staff):

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security

- The school is not responsible for the day to day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- Devices may not be used in tests or exams (including adults).
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Personal devices can be charged within school
- Devices must be in silent mode on the school site
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances (see handbook)
- Printing from personal devices will not be possible

6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Broadwater Church of England Primary School have been agreed

Signed by (SLT): 

Date: 26.06.2023

Date for review: July 2024

Acknowledgement

This template terms of reference document is based on one provided to schools by Somerset County Council

Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: [Report Harmful Content: Laws about harmful behaviours](#)

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about [“Cyber crime – preventing young people from getting involved”](#). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](#).

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they’re securely handling data.

- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers,

health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - <http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

[Harmful Sexual Support Service](#)

CEOP

CEOP - <http://ceop.police.uk/>

[ThinkUKnow](https://www.thinkuknow.co.uk/) - <https://www.thinkuknow.co.uk/>

Others

[LGfL – Online Safety Resources](#)

[Kent – Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

[SWGfL 360 Groups – online safety self review tool for organisations working with children](#)

[SWGfL 360 Early Years - online safety self review tool for early years organisations](#)

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -

<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

[Department for Education: Teaching Online Safety in Schools](#)

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Organisations](#)

[IRMS - Records Management Toolkit for Schools](#)

[ICO Guidance on taking photos in schools](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

SWGfL - [Cyber Security in Schools](#).

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[SWGfL – Online Safety Guidance for Parents & Carers](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

Childnet – [Trust Me](#)

Research

[Ofcom –Media Literacy Research](#)

[Ofsted: Review of sexual abuse in schools and colleges](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Glossary of Terms

AUP/AUA Acceptable Use Policy/Agreement – see templates earlier in this document

CEOP Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CPD Continuous Professional Development

FOSI Family Online Safety Institute

ICO Information Commissioners Office

ICT Information and Communications Technology

INSET In Service Education and Training

IP address The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider

ISPA Internet Service Providers' Association

IWF Internet Watch Foundation

LA Local Authority

LAN Local Area Network

MAT Multi Academy Trust

MIS Management Information System

NEN National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK Think U Know – educational online safety programmes for schools, young people and parents.

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

UKCIS UK Council for Internet Safety

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in September 2022. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.